

Searching PAJ

第1頁, 共2頁

PATENT ABSTRACTS OF JAPAN

RECEIVED
CENTRAL FAX CENTER

(11)Publication number : 2001-216046

JUN 20 2006

(43)Date of publication of application : 10.08.2001

(51)Int.Cl.

G06F 1/00
G06F 15/00

(21)Application number : 2000-371401

(71)Applicant : AVAYA TECHNOLOGY CORP

(22)Date of filing : 06.12.2000

(72)Inventor : THOMPSON JOHN S
THOMPSON MELINDA M

(30)Priority

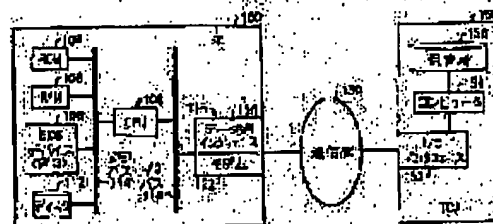
Priority number : 1999 454625 Priority date : 06.12.1999 Priority country : US

(54) DEVICE SECURITY MECHANISM BASED ON REGISTERED PASSWORD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a security mechanism based on a registered password.

SOLUTION: When a PC is booted, a security program is executed. The security program urges a user to input a password, and this is enciphered by a stored key, and the enciphered password is compared with the stored password. When those passwords are not coincident, the boot is abandoned, and the PC is invalidated. Only when those passwords are coincident, the boot is continued, and the use of the PC is authorized.



LEGAL STATUS

[Date of request for examination] 22.03.2002

[Date of sending the examiner's decision of rejection] 04.04.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-216046

(P2001-216046A)

(43) 公開日 平成13年8月10日 (2001.8.10)

(51) Int.Cl. ⁷	識別記号	F I	ページ数	ページ数
G 0 6 F 1/00	3 7 0	G 0 6 F 1/00	3 7 0 E	
15/00	3 3 0	15/00	3 3 0 E	

審査請求 未請求 請求項の数10 O L (全 10 頁)

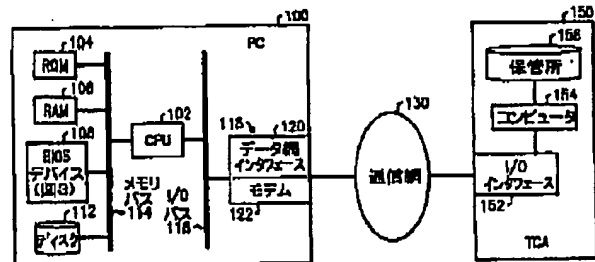
(21) 出願番号	特願2000-371401 (P2000-371401)	(71) 出願人	500500044 アバイア テクノロジー コーポレーション アメリカ合衆国, 07920 ニュージャージー, イ, パスキング リッジ, マウント エア リー ロード 211
(22) 出願日	平成12年12月6日 (2000.12.6)	(72) 発明者	ジョン エス. トンプソン アメリカ合衆国 80303 コロラド, ボー ルダー, エンボリア ロード 695
(31) 優先権主張番号	09/454625	(72) 発明者	メリンダ エム. トンプソン アメリカ合衆国 80303 コロラド, ボー ルダー, エンボリア ロード 695
(32) 優先日	平成11年12月6日 (1999.12.6)	(74) 代理人	100064447 弁理士 岡部 正夫 (外11名)
(33) 優先権主張国	米国 (U S)		

(54) 【発明の名称】 登録されているパスワードに基づくデバイス機密機構

(57) 【要約】 (修正有)

【課題】 本発明は、登録されているパスワードに基づくデバイス機密機構に関する。

【解決手段】 PCがブートされると、機密プログラムが実行される。機密プログラムは、ユーザにパスワードを催促し、これを格納されている鍵にて暗号化し、暗号化されたパスワードを格納されているパスワードと比較する。これらパスワードが一致しない場合は、ブートは、放棄され、PCは不能にされる。これらパスワードが一致した場合にのみ、ブートが継続され、PCの使用が許される。



(2)

特開2001-216046

【特許請求の範囲】

【請求項1】 デバイス機密装置であって、

パスワードを格納し、およびデバイスの使用が不能にされている間はデバイスのユーザが格納されているパスワードにアクセスすることができないようにするための前記デバイス内のメモリ；前記デバイスを外部エンティティに接続するコネクタ；前記デバイス内の、前記メモリと協力して、ロックに格納されているパスワードと対応するパスワードが与えられない限り、デバイスの使用を不能にするためのロック；および前記メモリ、コネクタ、およびロックと協力して、デバイスの使用が許され、前記外部エンティティへの接続が設定されたことに応答して、前記格納されているパスワードの変更を、前記格納されているパスワードが前記接続された外部エンティティによって格納されているパスワードと一致する場合は、許すとともに、前記外部エンティティによる前記変更されたパスワードの格納を実行するための手段の配列を備えることを特徴とするデバイス機密装置。

【請求項2】 前記メモリが、コンピュータのBIOSプログラムおよびパスワードを格納するためのBIOSデバイスから成ることを特徴とするコンピュータ用の請求項1記載の装置。

【請求項3】 前記コネクタが前記デバイスのネットワーク通信ポートから成り；前記エンティティが遠隔信託機関から成ることを特徴とする請求項1記載の装置。

【請求項4】 前記コネクタが前記デバイスの入力ポートから成り；前記エンティティがローカルメモリデバイスから成ることを特徴とする請求項1記載の装置。

【請求項5】 前記ロックが前記デバイスに電力が投入された際に行う格納されたプログラムから成ることを特徴とする格納プログラム制御方式のデバイス用の請求項1記載の装置。

【請求項6】 前記メモリが、前記コンピュータのBIOSプログラム、パスワード、およびロックプログラムを格納するためのBIOSデバイスから成ることを特徴とするコンピュータ用の請求項5記載の装置。

【請求項7】 前記手段の配列が：ユーザの識別を外部エンティティと協力して確立（検証）するための手段；格納されているパスワードを外部エンティティに供給するための手段、および前記外部エンティティからの前記確立（認証）された識別と供給されたパスワードが前記外部エンティティによって格納されている識別とパスワードと一致したことを示す指標の受信に応答して、前記格納されているパスワードの変更を実行するための手段を含むことを特徴とする請求項1記載の装置。

【請求項8】 前記手段の配列がさらに：前記ユーザからの新たなパスワードの受信に応答して、前記メモリ内に新たなパスワードを格納するとともに、前記新たなパスワードを格納のために前記外部エンティティに送信するための手段を含むことを特徴とする請求項7記載の装

置。

【請求項9】 前記メモリが、前記パスワードの暗号版および暗号鍵を格納し、

前記ロックが、非暗号化パスワードを受信すると、これに応答して、受信されたパスワードを格納されている暗号鍵にて暗号化し、この暗号版パスワードを前記格納されている暗号版パスワードと比較し、これら比較されたパスワードが一致しない場合は、前記デバイスの使用を不能にすることを特徴とする請求項1記載の装置。

【請求項10】 前記手段の配列が：ユーザの識別を外部エンティティと協力して確立（検証）するための手段；格納されている暗号版パスワードを前記外部エンティティに供給するための手段；前記外部エンティティからの前記確立（認証）された識別と供給されたパスワードが前記外部エンティティによって格納されている識別とパスワードと一致したことを示す指標の受信に応答して、前記格納されているパスワードの変更を実行するための手段、

外部エンティティから受信される新たな暗号鍵を前記メモリ内に格納するための手段、およびユーザから受信される新たなパスワードを格納されている新たな暗号鍵にて暗号化し、こうして暗号化された新たなパスワードを前記メモリ内に格納するとともに、暗号化された新たなパスワードを格納のために前記外部エンティティに送信するための手段を含むことを特徴とする請求項9記載の装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、一般的には、デバイスの窃盗あるいは無許可のアクセスを抑制するための機密機構、より詳細には、パスワード機構に関する。

【0002】

【従来の技術】 あらゆる種類の電子デバイスは、それらが典型的にサイズの割りに高い価値を有するために窃盗の標的となる。ポータブルコンピュータデバイス、例えば、ノート型コンピュータは、典型的には、小さく、高価で、持運びが楽であるために、特に、盗難に遇い易い。従来の機密対策は、アンカリングデバイスおよびロックエンクロージャを使用する物理的抑止力に基づく。ただし、これらは、運搬性および使用の利便性を制限する。デバイスを所有者以外には使用できないようにし、この事実について宣伝したなら、これらは泥棒にとっては価値を失い、このため、窃盗の対象とはなくなることが期待できる。これは、暗に簡単には突破することができないある種のパスワードシステムの使用を示唆する。ただし、従来のパスワード機構では不十分である。

【0003】 今日のポータブルコンピュータにおいては、アクセスを制限するためにソフトウェアベースのパスワードシステムが用いられている。ただし、これらは、オペレーティングシステムソフトウェアを再実装す

(3)

特開2001-216046

ることで、あるいは、あるケースにおいては、より単純な操作、例えば、これらをサポートするオペレーティングシステム（例えば、Windows 95における“Safe Mode”）内のループホールに不当に働き掛けることで突破することができる。それにもかかわらず、コンピュータに電力を投入する際にパスワードを供給する方法は、ユーザの正当性をチェックするための最も簡単なやり方である。ハードウェアベースの機密システム（例えば、幾つかのカーラジオ上に搭載されている機密システム）もパスワードによる制御をサポートする。ただし、パスワードが失われた場合は、このデバイスを再び使用できるようにするためには、大変なハードウェアの外科的手術（解体修理）に頼るしかない。パスワードシステムの突破に対するコストおよび労力の両面での障壁を設ける必要があるが、同時に、パスワードが失われた際の扱いが容易であり、しかも、ある機関によってデバイスの正当性を確認できることも要望される。現在、公開暗号署名（Public Encrypted Signatures）が受信された情報がユーザによって合法的に供給されたものであるか検証するために用いられている。割当てられた公開鍵を用いてのパスワードの符号化および暗号化はある人が一意に登録されたデバイスを扱っていることを保障するための手段として用いることができる。信託証明機関（Trusted Certification Authorities, TCA）も存在し、これは、登録されたデジタル署名を提供し、ユーザの登録情報を管理する。これら機関はメッセージの符号化のための署名を登録するために用いることができる。ただし、これら現存の能力（機能/機関）のどれも、そのみでは携帯デバイスに対する十分な機密機構を提供することはできない。

【0004】

【発明が解決しようとする課題】本出願人は、携帯デバイスに対する機密システムには以下に示すような幾つかの要件が存在することを認識した：

- ・機密システムは、パーツあるいは製造において、デバイスにあまり大きなコストを追加すべきではなく、できればコストを全く追加すべきではなく、また流通システムにも追加の負担を掛けるべきではない。
- ・機密システムを突破するための労力もしくは金銭面での費用がデバイスの価値に接近あるいはこれを超過する必要がある。
- ・デバイスへのアクセスは所有者に個人化され、しかも大きな困難なしに所有権の譲渡が可能である必要がある。
- ・機密システムは、現存のハードウェア、ソフトウェアおよび機密技術を使用し、好ましくは、現存のコンピュータ上への実装に適したものである必要がある。
- ・機密システム内で使用される個人的な情報はデバイスへの正当なアクセスを再設定することが必要となったとき支援することができるある機関によって保管できる必

要がある。

・機密システムは標準となるのに十分に魅力的であり、デバイスの販売業者と第三者の両方によって経済的にサポートできる必要がある。

【0005】

【課題を解決するための手段】従って、本発明は、従来の技術のこれら問題および短所を解決するため、および従来の技術の要件を満たすことに向けられる。概略的には、本発明によると、デバイス機密装置は、以下の要素から構成される。第一は、デバイス内の、パスワードを格納するためのメモリである。このメモリは、これが、デバイスのユーザが、デバイスの使用が不能にされている場合は、格納されているパスワードにアクセスすること（つまり、これを抽出および／あるいは変更すること）を防止する意図で機密であることを要求される。このようなメモリの一例としては、パーソナルコンピュータのBIOSプログラムを格納するBIOSデバイスがある。もう一つの要素は、デバイスを外部エンティティ、例えば、ローカルメモリデバイスもしくは遠隔信託機関に接続するためのコネクタである。このようなコネクタの一例としては、パーソナルコンピュータの入／出力ポートおよびネットワーク通信ポートが含まれる。もう一つの要素は、デバイス内の、メモリと協力して、デバイスの使用を、格納されているパスワードに対応するパスワードがロックに供給されない限り、不能にするロックである。このロックは、一つの実施例においては、機密メモリ、例えば、BIOSデバイス内にパスワードとともに存在するプログラムとして実現される。もう一つの要素は、メモリ、コネクタ、およびロックと協力して、デバイスの使用が許され、外部エンティティへの接続が設定されたことに応答して、格納されているパスワードが接続された外部エンティティによって格納されているパスワードと一致したとき、格納されているパスワードの変更を許すとともに、外部エンティティによる変更されたパスワードの格納を実行するための手段の配列である。この手段の配列は、一つの実施例においてはプログラムとして実現されるが、ただし、これは必ずしも機密デバイスに格納される必要はない。

【0006】本発明は、

【発明が解決しようとする課題】のセクションにおいて指摘された幾つかのあるいは全ての要件が満たされるように実現される。これら要件には上述のように以下が含まれる：

1. 製造過程において、他のソフトウェアをインストールするために非機密始動モードを選択できる要件。
2. 機密システムの突破には、デバイスを解体し、機密メモリ（例えば、コンピュータのBIOSメモリ）を物理的に切り離し、書きなおすことが要求される要件。これは、簡単で安価な仕事ではない。
3. デバイスの所有権を個人化するばかりではなく、こ

(4)

特開2001-216048

れを安全に譲渡もしくは変更できる要件。

4. 新たな技術を必要としないという要件。実際、本発明の機能は、現存の知能デバイス、例えば、コンピュータに追加することもできる。

5. 信託機関を、機密を管理および制御するため、および価値あるサービスを提供するために使用できるという要件。信託機関の代わりに、信託機関の代わって機能し、システムのよりローカルなバージョンを提供するために、PCカードのようなローカルプラグインデバイスを使用することもできる。

6. 本発明は、上述の全ての要件を満たすように実現できるために、本発明は標準としておよび/あるいは広く展開された商業的機能として魅力的である。本発明のこれらおよびその他の特徴および長所が、本発明の実施例の以下の説明を図面を参照しながら読むことで一層明白になるものである。

【0007】

【発明の実施の形態】図1は、ポータブルコンピュータ(PC)100を示す。ポータブルコンピュータ(PC)100は、中央演算ユニット(CPU)102、読出専用メモリ(ROM)104、ランダムアクセスメモリ(RAM)106、ベーシック入/出力オペレーティングシステム(BIOS)デバイス108、およびディスクメモリ112を備え、これら全てがメモリバス114によって相互接続される。ポータブルコンピュータ(PC)100は、さらに、入/出力(I/O)インタフェース116を備え、これは、データ網インタフェース120および/あるいはモデム122から成り、入/出力(I/O)バス118によって中央演算ユニット(CPU)102に接続される。図2には、入/出力(I/O)インタフェース116が入/出力(I/O)ポート220から成るポータブルコンピュータ(PC)100の代替の形態が示される。上の説明までは、ポータブルコンピュータ(PC)100は従来のものである。ポータブルコンピュータ(PC)100は、BIOSデバイス108のようなメモリ要素：すなわち、その内容がデバイスの動作が不能にされている際はデバイスのユーザによって容易にアクセス(抽出もしくは変更)すること、あるいはバイパスすることは不可能であり、その動作能力がこれらの内容に依存するメモリ要素をもつ任意のデバイスであり得る。

【0008】BIOSデバイス108は、不揮発性の“永久(permanent)”メモリから成り、この内容は、電力が不在のときも保存される。ただし、読出専用メモリ(ROM)104とは異なり、これは、特別なソフトウェアの制御の下で、電気的に変更およびプログラムが可能であり、ポータブルコンピュータ(PC)100の寿命を通じてBIOS108を更新することができる。このタイプのメモリデバイスは、プログラム可能読出専用メモリ(PROM)、電気的消去可能PROM(EEP

ROM)もしくはフラッシュメモリとして知られている。ポータブルコンピュータ(PC)100がブートされると、例えば、電力が投入されると、中央演算ユニット(CPU)102が読出専用メモリ(ROM)104からのインストラクションの実行を開始する。これらのインストラクションは、中央演算ユニット(CPU)102に対して、BIOS108の内容(BIOSプログラム)をランダムアクセスメモリ(RAM)106内に転送し、ランダムアクセスメモリ(RAM)106からのこれらの内容を実行するように指令する。BIOSプログラムの実行によってポータブルコンピュータ(PC)100がブートされる。ポータブルコンピュータ(PC)100は、BIOSプログラムなしではブートすることはできない。そして、もし、ポータブルコンピュータ(PC)100がブートできない場合は、BIOSプログラムは更新することと変更することとできない。このため、BIOSデバイス108の内容が“コラプト(corrupted)”した場合は、BIOSデバイス118を交換するか、ポータブルコンピュータ(PC)100を製造業者にもってゆき、BIOSデバイス108への通常の電気接続を物理的にバイパスし、これを再プログラムすることが必要となる。これも従来のやり方である。

【0009】図3は、BIOSデバイス108の内容を示す。本発明によると、BIOSデバイス118は、窃盗抑止のための機密機構を実装する。従来のBIOSプログラム300を含むことに加えて、BIOSデバイス108は、暗号鍵304およびパスワード306の項目を含む機密プログラム302も含む。機密プログラム302は、BIOSプログラムの先頭に付加され、ブート時に、これがランダムアクセスメモリ(RAM)106内に、BIOSプログラム300の前にあるいはこれとともにロードされ、BIOSプログラムの実行が完結される前に実行される。

【0010】機密機構の基本概念は、BIOSデバイス108内に一意なパスワード306を格納しておき、各ブート(例えば、電力の投入)サイクルの最初に、ブートサイクルおよびその後のポータブルコンピュータ(PC)100の動作を続けるためには、キーボードあるいは他のI/Oデバイスから入力されたパスワード306がこれと一致することを要求することにある。パスワード306の不一致は、機密的には、BIOSプログラム300の“コラプト(corrupt)”と等価となる。このため、ポータブルコンピュータ(PC)100は、パスワード306をもたないものによってはなんの役にも立たなくなる。そして、この機密機構を出し抜くことは非常に困難である。これには、BIOSデバイス108を新たなものと交換するか、ポータブルコンピュータ(PC)100を製造業者にもってゆき、BIOSデバイス108への通常の電気的接続を物理的にバイパスし、これを再プログラムすることが必要となる。このため、ポ

(5)

特開2001-216046

ータブルコンピュータ（PC）100を盗むことは経済的な価値がなくなり、このため窃盗の抑止となる。

【0011】一方において、機密機構は、これを出し抜くもしくは突破することが努力に値しなくなるのに十分にロバスト（頑丈）であることが要求され、他方においては、この機密機構は、パスワードを忘れてしまった場合にもマシンの使用を回復でき、または、パスワードを見破られたり、マシンが合法的に人手に渡った場合でも、機密を回復できるように十分に柔軟であることが要求される。この目的のために、TCA（trusted certification authority：委託証明機関）150の概念が導入される（図1参照）。

【0012】TCA150は、パスワードの保管所であるとともに、パスワードの維持に対するサービスでもある。これは、例えば、ポータブルコンピュータ（PC）100の製造業者もしくは販売業者による顧客へのサービスとして、あるいは第三者による有料加入サービスとして提供される。図1に示すように、TCA150は、TCA150とPC100が通信することを可能にする通信網130（例えば、データ網もしくは電話網）への入/出力（I/O）インタフェース152、TCAサービスプログラムを実行するコンピュータ154、およびパスワードおよび関連する情報を格納するための保管所156（例えばデータベース）から構成される。

【0013】図2に示す代替の実施例においては、中央TAC150が省かれ、各PC100に、TCA一代用機能をその対応するPCのみに提供する機密カード250が設けられる。機密カード250は、PC100のI/Oポート220と着脱可能に噛み合う（例えば、これらプラグインされる）I/Oポート252とメモリ254から構成される。これは、一例においては、PCMCIAカードあるいはフロッピー（登録商標）ディスクから成る。

【0014】新しく製造されたPC100は、これがその内部に搭載された有効なパスワードをもたず、パスワード306がナル値であるという意味で機密ではない。このように機密でないモードにあるために、PC100は、工場においてなんの障害もなく、ソフトウェアにて初期化し、テストすることができる。さらに、PC100は、有効なパスワードなしに販売することもできる。ただし、PC100は、エンドユーザに販売する前のPC100の窃盗を抑止するために、工場から出荷する前に有効なパスワード306にてプログラムしておここともできる。後者の場合は、販売の時点でパスワードを顧客に伝えることともに、パスワード306あるいはPC100の所有者を識別する情報をTCA150の保管所156内に入力しておくか、できるだけ早くパスワード306を機密カード250のメモリ156内に入力することが必要となる。

【0015】図4～図6は、機密プログラム302の機能を示す。例えば、電力が投入されたために、ステップ400において、BIOSデバイス108の内容の実行が開始されると、CPU102は、ステップ401において、PC100のディスプレイおよびキーボードを起動する。殆どのBIOSプログラム300は、基本的なディスプレイおよびキーボードドライバを備えるために、ステップ401は、通常は、BIOSプログラム300のディスプレイおよびキーボードを起動する部分を実行することから成る。キーボードおよびディスプレイを動作を起動しないBIOSプログラム300の場合は、ステップ401は、機密プログラム302の基本的なディスプレイおよびキーボードドライバを含む部分、あるいはディスクからディスプレイおよびキーボードドライバをロードし、これらを起動する部分を実行することから成る。次に、ステップ402において、CPU102が、プログラム302を実行し、最初に、パスワード306をチェックし、その値がナルであるか否か決定する。この値がナルでない場合は、PC100は、機密モードにて動作しており、このため、CPU102は、ステップ404において、PC100のユーザにパスワードを入力するように催促する。これは、例えば、PC100のディスプレイ画面にこの効果のためのプロンプトを表示することによって行なわれる。ユーザがこれに応答すると、例えば、PC100のキーボードを用いてパスワードをタイプ入力すると、CPU102は、ステップ406において、受信されたパスワードを格納されている暗号鍵304にて暗号化し、次に、ステップ408において、暗号化された受信されたパスワードを、これも暗号鍵304にて暗号化されたパスワード306と比較し、それらが一致するか決定する。これらが一致しない場合は、ステップ410において、PC100のブートおよびそれ以上の動作を中止し、PC100を使用できないようにする。これらが一致した場合は、PC100は、安全であり、このため、ステップ411において、PC100のブーティングを完結させる。ただし、制御を放棄する前に、ステップ412において、プログラム302は、CPU102に対して、ユーザにパスワードの変更を希望するか尋ねることを指令する。ステップ412においてユーザがパスワードの変更を希望しないことが決定された場合は、PC100は、ステップ420において、従来のやり方で、ただし、機密モードにて動作を継続する。

【0016】ステップ402に戻り、ここでパスワード306がナルであることが決定された場合は、これは、PC100が非機密モードにて動作していることを意味し、このため、CPUは、ステップ415において、ブーティングを完結させる。ただし、制御を放棄する前に、プログラム302は、ステップ416において、CPU102に対して、ユーザに有効なパスワードの設定を催促するように指令する。ステップ418においてユ

(6)

特開2001-216046

ユーザがパスワードの設定を選択しないことが決定された場合は、PC100は、ステップ420において、従来のやり方で非機密モードにて動作を継続する。

【0017】機密機構が突破されないようにするためには、PCの動作能力を起動あるいは不能にする（制御する）機密ゲートウェイもしくはロックを構成する機密プログラム302のステップ402～410のみをバイパスあるいは突破から保護することで十分である。従って、プログラム302のこの部分のみが、パスワード306および暗号鍵304とともに、機密メモリ、例えば、BIOSデバイス108内に格納される。その後は、機密ゲートウェイは、パスワード306の値がナルの場合、もしくは正しいパスワードが入力された場合に通過できる。いずれの場合も、ユーザは、現在、PC100を所望のやり方で自由に用いることができる。従って、プログラム302の、単にパスワード306の変更（初期設定も含む）を制御する残りの部分は、CPU102によってアクセスできるPC100の任意の他の部分に格納することができる。例えば、フロッピーディスクがディスクドライブ内に存在する場合は、BIOSプログラム300は、PCにおいて通常行なわれるようにこれからブートすることを試み、このため、プログラム302の残りの部分はフロッピーディスク上に格納され、この時点で、パスワード306を設定もしくは修正するために実行される。後に説明するように、パスワードの維持は、BIOSデバイス108の二つの項目304と306のみが変更される点とPC100の外部への通信が行なわれる点を除いて、機能的にはBIOSプログラム300のグレードアップあるいは変更と差はない。

【0018】図面に戻り、図4のステップ414においてユーザがパスワードの変更を選択した場合、あるいはステップ418においてパスワードの設定を選択した場合は、CPU102は、図5におけるTCA150あるいは図6における機密カード250との対話へと進む。最初に、図5に進み、CPU102は、ステップ424において、従来のやり方で、TCA150への接続を網インタフェース120およびデータ網130（例えば、LANもしくはインターネット）あるいはモデム122および電話網130を介して設定する。TCA150の必要なアドレスは、機密プログラム302の一部として格納されるか、あるいは、ステップ422において、CPU102がユーザにアドレスを供給するように催促することで得られる。ステップ250において接続が設定されると、ステップ426と452において、PC100とTCA150が協力して、発呼ユーザの識別を確立（検証）する。例えば、TCA150が網130を介してユーザに質問し、ユーザがPC100を介してこれらに答え、TCA150が、これら答えを保管所内に格納してあるそのユーザに関する情報と比較し、一致が見ら

れるか決定する。別の方法として、ステップ426と452は、現存のパスワードの変更の場合は省略することもできる。ユーザの識別がTCA150を満足させるように確立（認証された）場合は、TCA150は、ステップ454において、PC100の格納されている暗号版パスワード306を要求し、CPU102は、これに応じて、ステップ428において、パスワード306を検索し、これを送り返す。受信されたパスワードが、ステップ455において、ナルでないことが決定された場合は、TCA150はステップ456において、保管所156を探索し、このパスワードおよびこれと対してこれと関連して格納されているユーザの識別を含む任意の情報を見つめる。保管所156内にパスワードが見つかった場合は、TCA150は、ステップ458において、そのペアの情報がステップ452において決定された発呼ユーザの識別と一致するか決定する。格納されている識別と発呼ユーザの識別が一致しない場合は、TCA150は、ステップ460において、PC100にその通知およびやりとりの拒否を送信し、ステップ462において、PC100への接続を切ることでこのやりとりを終了する。代替として、（パスワードの変更であり）ステップ426と452が逆行されない場合は、TCA150は、単に、ステップ456において、受信されたパスワードを求めて保管所156を探索し、ステップ458において、保管所156内にそのパスワードが存在するかチェックする。CPU102が、ステップ430において、そのやりとりが拒否されたことを決定した場合、CPU102は、ステップ432において、パスワードの変更を行なうことなく、従来の動作を継続する。別の方法として、CPU102は、ステップ432において、ブートアップを否定し、PC100を停止し、こうして、PC100を使用ではないようにすることもできる。

【0019】ステップ458において、発呼ユーザの識別がこのPC100のパスワード306としてTCA150によって格納されているユーザの識別と一致することが見つかった場合、もしくは、ステップ455において、受信されたパスワードがナルであることが見つかった場合は、TCA150は、ステップ466において、新たなプライベート／公開暗号鍵ペアを生成し、ステップ468において、このペアの公開暗号鍵をPC100に送信する。CPU102は、ステップ436において、この公開暗号鍵を受信し、ステップ438において、これを、BIOSデバイス108の暗号鍵304内に格納し、このプロセス内の暗号鍵304の以前の値を無効にする。CPU102は、次に、ステップ440において、ユーザに新たなパスワードを催促し、これを受信すると、ステップ442において、この新たなパスワードを格納されている暗号鍵304にて暗号化する。BIOSデバイス108をプログラミングするための従来の

(7)

特開2001-216046

の専用のソフトウェアの制御下において、CPU102は、次に、ステップ444において、新に暗号化されたパスワードをBIOS108のパスワード306内に格納し、このプロセスにおけるパスワード306の以前の値を無効にする。幾つかのBIOSデバイスは、その内容を変更するためには、全デバイスを無効にすることを要求することがあり、この場合は、TCA150が全BIOSデバイスに新たな暗号鍵とパスワードをもつ内容を供給するか、もしくは、CPU102が、BIOSデバイスの内容を読み出し、そのイメージを生成し、そのイメージ内の暗号鍵およびパスワードを変更し、その後、変更されたイメージを再びBIOSデバイス内に書き込むことが必要となる。このため、CPU102は、ステップ446において、新たな暗号版パスワードをTCA150に送信する。PC100は、次に、ステップ448において、従来の動作に進む。TCA150は、ステップ470において、新たな暗号版パスワードを受信し、ステップ472において、これと新に生成された暗号鍵ペアのプライベート鍵を、保管所156内に、発呼者識別情報と関連する以前のパスワードと鍵の代わりに、格納する。TCA150は、次に、ステップ474において、その動作を終了する。

【0020】ユーザが万一パスワードを忘れてしまった場合は、ユーザは、これをTCA150の助けを借りて検索することができる。例えば、ユーザは、TCA150の運用者に電話を掛け、ステップ426と452のやり方で、運用者に対してユーザの識別を確立する。保管所156内に格納されているユーザに関する情報にはユーザの声紋が含まれ、運用者は、この声紋と電話のユーザの音声とを用いて、ユーザを認証することができる。いったんユーザが認証されると、運用者は、コンピュータ154に対して、ユーザのパスワードを解読するように指令する。コンピュータ154は、これを、保管所156からユーザの暗号版パスワードおよびプライベート暗号鍵を探索し、プライベート鍵を用いてこのパスワードを解読することによって行なう。運用者は、次に、解読されたパスワードを呼を介してユーザに報告し、同時に、呼が機密でない場合は、できる限り早くパスワードを変更するように警告する。

【0021】PC100のユーザが、図2の実施例の場合のように、機密カード250を搭載する場合は、ステップ413においてパスワードの変更が選択された場合、もしくはステップ418においてパスワードの設定が選択された場合、CPU102は、図6に示すやり方で、機密カード250との対話を開始する。最初に、CPU102は、ステップ600において、I/Oポート220内に機密カード200が存在するかチェックする。機密カード250がI/Oポート220に接続されていない場合は、CPU102は、ステップ602において、PC100のユーザに接続することを催促し、次

に、ステップ600に戻る。ステップ600において、機密カード250がI/Oポート220に接続されていることが決定された場合は、CPU102は、オプションとして、ステップ604～608において、別のデバイスに対するパスワードを誤って破壊することを防止するために、それがこのPC100に対して正しい機密カードであるか否かチェックする。このチェックを遂行するために、CPU102は、ステップ604において、機密カード250からメモリ254の内容を検索し、ステップ606において、これら内容をパスワード306と比較し、それらが一致するか調べる。一致しない場合は、CPU102は、ステップ608において、ユーザに対して、正しい機密カード250をPC100に接続するように催促し、その後、ステップ600に戻る。CPU102がステップ606において正しい機密カード250がPC100に接続されていることを見つけた場合、もしくは機密カード250が正しいものであるかチェックするためのステップ604～608が省略される場合は、CPU102は、ステップ610において、ユーザに新たなパスワードを催促し、これを受信する。CPU102は、次に、ステップ612において、暗号鍵304を用いて、この新たなパスワードを暗号化する。公開鍵の暗号化は、TCA150などの遠隔機関は存在しないために不要である。オプションとして、例えば、殆どのUNIX（登録商標）オペレーティングシステム環境において通常見られるように、全てのPC100内に共通の鍵を用いることもできる。BIOSデバイス108をプログラミングするための従来の専用のソフトウェアの制御下において、CPU102は、次に、ステップ614において、新に暗号化されたパスワードを、BIOSデバイス108内にパスワード306として格納する。CPU102は、さらに、ステップ616において、これを、機密カード250のメモリ254内に、ここに格納されている以前の内容の代わりに、格納する。図5のステップ444の場合と同様に、機密カード250は、全BIOSデバイス108の内容を新たなパスワードとともに供給することが必要とされる場合がある。代替もしくは追加として、CPU102は、機密カード250のメモリ254内に非暗号化パスワードを格納することもできる。この方法は、ユーザが万一パスワードを忘れてしまった場合でも、ユーザがこれを機密カード250からコンパティブルなI/Oポート220をもつ別のマシンを介して検索できる（読み出しおよび/あるいは表示できる）という長所をもつ。ただし、これは、ユーザが機密カード250を、PC100とは別個に、物理的に機密に保つことを期待できることを仮定する。CPU102は、その後、従来のやり方で動作を継続する。勿論、当業者においては明らかなように上述の実施例に対する様々な変更および修正が可能である。例えば、本発明は、様々な異なるデバイス上に、ある一つの

(8)

特開2001-216046

実現の機密が突破された場合でも全てのデバイスが影響を受けることがないように異なるやり方にて（例えば、製造業者に特定な、さらに、モデルに特定なやり方にて）実現することもできる。この目的に対しては、デバイス（PC）の通し番号がROM104内に格納され、これが製造業者および／あるいはモデルを識別するために用いられる。これら変更および修正は、本発明の精神および範囲から逸脱することも、本発明の付随する長所を低減することもなく、実施することが可能であり、従って、これら変更および修正も、従来の技術によって制限されない限り、特許請求の範囲内に含まれるものである。

【図面の簡単な説明】

【図1】 本発明の第一の実施例を含むコンピュータ網のブロック図である。

【図2】 本発明の第二の実施例を含むコンピュータ網のブロック図である。

【図3】 図1および図2のポータブルコンピュータのBIOSデバイスの内容のブロック図である。

【図4】 一体となって、図1および図2のポータブルコンピュータの機密プログラムの動作の機能流れ図である。

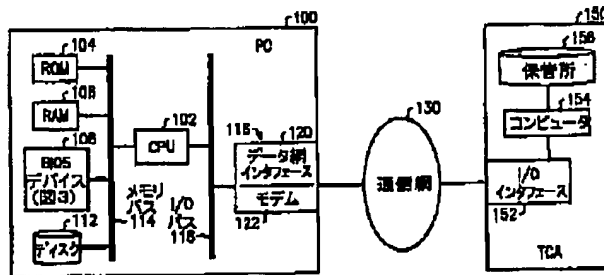
【図5】 図1のコンピュータ網の信託証明機関の動作の機能流れ図である。

【図6】 一体となって、図1および図2のポータブルコンピュータの機密プログラムの動作の機能流れ図である。

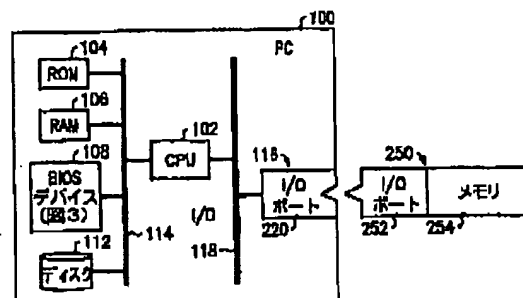
【符号の説明】

- 100 ポータブルコンピュータ（PC）
- 102 中央演算ユニット（CPU）
- 104 読出専用メモリ（ROM）
- 106 ランダムアクセスメモリ（RAM）
- 108 ベーシック入／出力オペレーティングシステム（BIOS）デバイス
- 112 ディスクメモリ
- 114 メモリバス
- 116 入／出力（I/O）インタフェース
- 118 入／出力（I/O）バス
- 120 データ網インタフェース
- 122 モデム
- 130 通信網
- 150 TCA（委託証明機関）
- 152 入／出力（I/O）インタフェース
- 154 コンピュータ
- 156 保管所
- 200 入／出力（I/O）ポート
- 250 機密カード
- 252 I/Oポート
- 254 メモリ
- 300 BIOSプログラム
- 302 機密プログラム
- 304 暗号鍵
- 306 パスワード

【図1】



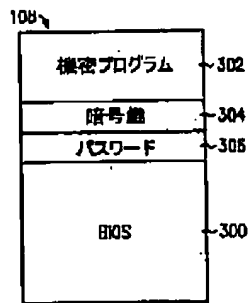
【図2】



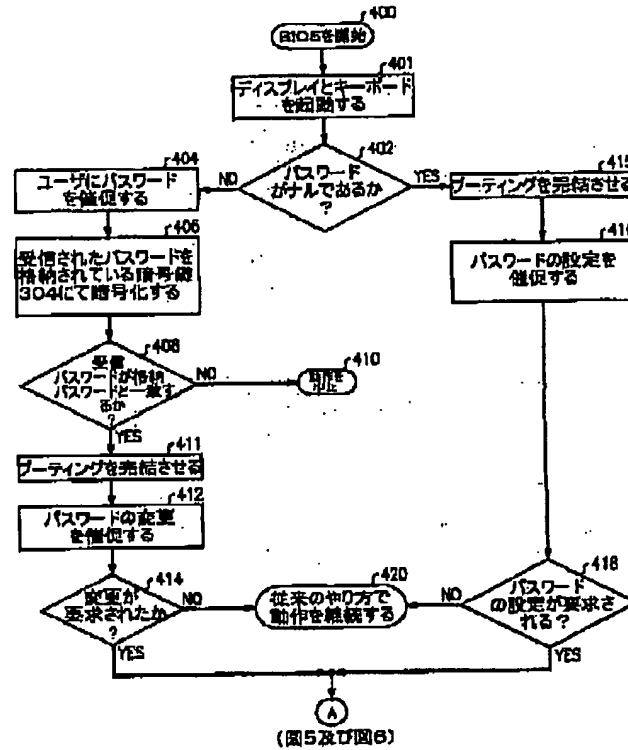
(9)

特開2001-216046

【図3】



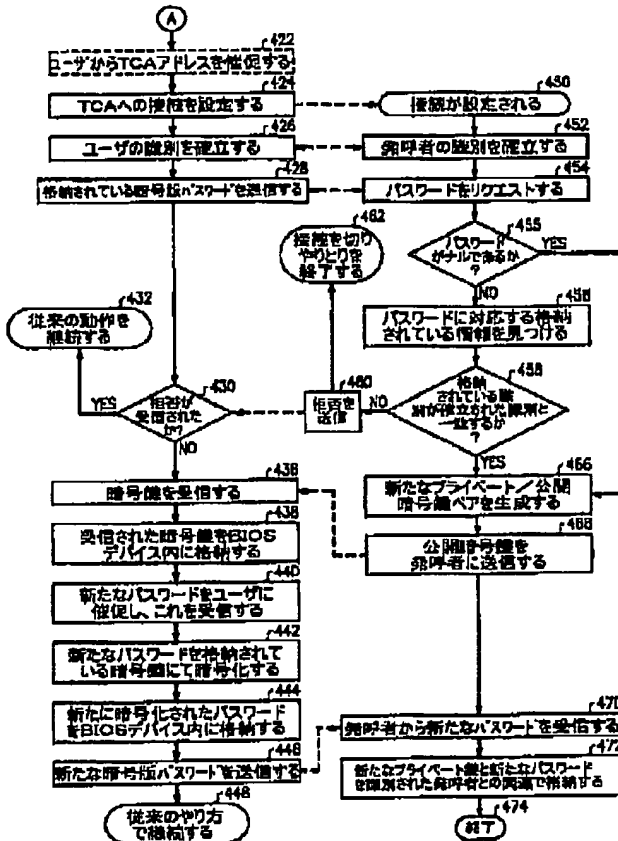
【図4】



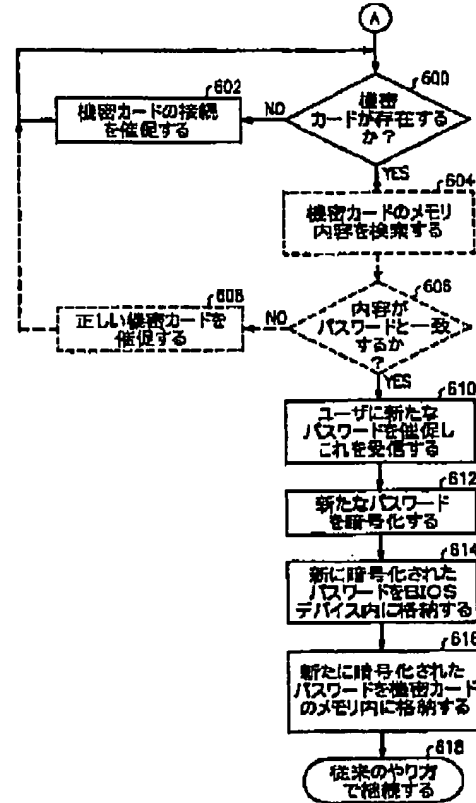
(10)

特開2001-216046

【図5】



【図6】



(11)

特開2001-216046

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第3区分

【発行日】平成14年6月26日(2002. 6. 26)

【公開番号】特開2001-216046(P2001-216046A)

【公開日】平成13年8月10日(2001. 8. 10)

【年通号数】公開特許公報13-2161

【出願番号】特願2000-371401(P2000-371401)

【国際特許分類第7版】

G06F 1/00 370

15/00 330

【F1】

G06F 1/00 370 E

15/00 330 E

【手続補正書】

【提出日】平成14年3月22日(2002. 3. 22)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 デバイスセキュリティ装置であって、パスワードを格納し、およびデバイスの使用が不能にされている間はデバイスのユーザが格納されているパスワードにアクセスすることができないようにするための前記デバイス内のメモリ；

前記デバイスを外部エンティティに接続するコネクタ；前記デバイス内の、前記メモリと協力して、ロックに格納されているパスワードと対応するパスワードが与えられない限り、デバイスの使用を不能にするためのロック；および

前記メモリ、コネクタ、およびロックと協働する配列であって、デバイスの使用が許され、前記外部エンティティへの接続が設定されたことに応答して、前記格納されているパスワードの変更を、前記格納されているパスワードが前記接続された外部エンティティによって格納されているパスワードと一致する場合は、許すとともに、前記外部エンティティによる前記変更されたパスワードの格納を実行するための配列を備えることを特徴とするデバイスセキュリティ装置。

【請求項2】 前記メモリが、コンピュータのBIOSプログラムおよびパスワードを格納するためのBIOSデバイスから成ることを特徴とするコンピュータ用の請求項1記載の装置。

【請求項3】 前記コネクタが前記デバイスのネットワーク通信ポートから成り；

前記エンティティが遠隔信託機関から成ることを特徴と

する請求項1記載の装置。

【請求項4】 前記コネクタが前記デバイスの入力ポートから成り；前記エンティティがローカルメモリデバイスから成ることを特徴とする請求項1記載の装置。

【請求項5】 前記ロックが前記デバイスに電力が投入された際に行う格納されたプログラムから成ることを特徴とする格納プログラム制御方式のデバイス用の請求項1記載の装置。

【請求項6】 前記メモリが、前記コンピュータのBIOSプログラム、パスワード、およびロックプログラムを格納するためのBIOSデバイスから成ることを特徴とするコンピュータ用の請求項5記載の装置。

【請求項7】 前記の配列が：ユーザの識別を外部エンティティと協力して確立するための手段；

格納されているパスワードを外部エンティティに供給するための手段、および前記外部エンティティからの前記確立された識別と供給されたパスワードが前記外部エンティティによって格納されている識別とパスワードと一致したことを示す指標の受信に応答して、前記格納されているパスワードの変更を実行するための手段を含むことを特徴とする請求項1記載の装置。

【請求項8】 前記配列がさらに：

前記ユーザからの新たなパスワードの受信に応答して、前記メモリ内に新たなパスワードを格納するとともに、前記新たなパスワードを格納のために前記外部エンティティに送信するための手段を含むことを特徴とする請求項7記載の装置。

【請求項9】 前記メモリが、前記パスワードの暗号版および暗号鍵を格納し、

前記ロックが、非暗号化パスワードを受信すると、これに応答して、受信されたパスワードを格納されている暗号鍵にて暗号化し、この暗号版パスワードを前記格納されている暗号版パスワードと比較し、これら比較されたパスワードが一致しない場合は、前記デバイスの使用を

(12)

特開2001-216046

不能にすることを特徴とする請求項1記載の装置。

【請求項10】 前記手段の記列が：

ユーザの識別を外部エンティティと協力して確立するための手段；

格納されている暗号版パスワードを前記外部エンティティに供給するための手段；

前記外部エンティティからの前記確立された識別と供給されたパスワードが前記外部エンティティによって格納されている識別とパスワードと一致したことを示す指標の受信に応答して、前記格納されているパスワードの変

更を実行するための手段、

外部エンティティから受信される新たな暗号鍵を前記メモリ内に格納するための手段、および

ユーザから受信される新たなパスワードを格納されている新たな暗号鍵にて暗号化し、こうして暗号化された新たなパスワードを前記メモリ内に格納するとともに、暗号化された新たなパスワードを格納のために前記外部エンティティに送信するための手段を含むことを特徴とする請求項9記載の装置。